I was already running freeciv-qt under gdb. I know the executable is named freeciv-qt-dev, but this was actually 2.6.1+. I went to Load Game, but then changed my mind, and the SEGV happened as I clicked Cancel. I can't repeat it.

```
Thread 1 "freeciv-qt-dev" received signal SIGSEGV, Segmentation fault.

nation_plural_for_player (pplayer=0x555559db0e60) at name_translation.h:123
123      return ptrans->translated;
(gdb) bt
#0  nation_plural_for_player (pplayer=0x555559db0e60) at name_translation.h:123
#1  0x00005555555d7e7c in show_new_turn_info() () at hudwidget.cpp:1664
#2  0x00005555555fb0c3 in qt_start_turn() () at menu.cpp:78
#3  0x00005555555e3601 in qtg_update_timeout_label() () at mapview.cpp:1086
#4  0x0000555555640616 in disconnect_from_server () at clinet.c:307
#5  0x000055555556e979ee in fc_client::slot_disconnect() (this=0x5555555fe2270) at fc_client.cpp:497
#6  0x00007fff71085c8 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#7  0x00007fff61dd236 in QAbstractButton::clicked(bool) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#8  0x00007fff61dd45e in () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#9  0x00007fff61daeb3a in () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#10 0x00007fff61daea65 in QAbstractButton::mouseReleaseEvent(QMouseEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#11 0x00007fff6166b04e in QWidget::event(QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#12 0x00007fff6162a868 in QApplicationPrivate::notify_helper(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#13 0x00007fff61630535 in QApplication::notify(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#14 0x00007fff6170da9a in QCoreApplication::notifyInternal2(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#15 0x00007fff61631157 in QApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QWidget*, QWidget**, QPointer<QWidget>&, bool, bool) ()
   at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#16 0x00007fff6168714d in () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#17 0x00007fff616899fdc in () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#18 0x00007fff6162a868 in QApplicationPrivate::notify_helper(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#19 0x00007fff61630535 in QApplication::notify(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#20 0x00007fff6170da9a in QCoreApplication::notifyInternal2(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#21 0x00007fff6174c4d73 in QGuiApplicationPrivate::processMouseEvent(QWindow*, QMouseEvent*, QWidget*, QWidget*, QWidget*, QPointer<QWidget>&, bool, bool) ()
   at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#22 0x00007fff6174c65fb in QGuiApplicationPrivate::processWindowSystemEvent(QWindowSystemInterfacePrivate::WindowSystemEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#23 0x00007fff6174a026b in QWindowSystemInterface::sendWindowSystemEvents(QFlags<QEventLoop::ProcessEventsFlag>) () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#24 0x00007fff617812e8 in () at /usr/lib/x86_64-linux-gnu/libQt5XcbQpa.so.5
#25 0x00007fff61f7584d in g_main_context_dispatch () at /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0
#26 0x00007fff61f758ad in () at /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0
#27 0x00007fff61f758b3 in g_main_context_iteration () at /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0
#28 0x00007fff61f7346a5 in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#29 0x00007fff6170db63b in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#30 0x00007fff6170e33a6 in QCoreApplication::exec() () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#31 0x00007fff6155555568e8e1 in fc_client::fc_main(QApplication*) (this=0x5555555fe2270, qapp=0x5555555b90380) at fc_client.cpp:257
#32 0x00007fff6155555556d3 in qtg_ui_main(2, char**) (argc=0x7fffffffbc8, argv=<optimized out>) at gui_main.cpp:191
#33 0x00007fff61555555639f8 in client_main (argc=1, argv=0x7fffffffbc8) at client_main.c:685
#34 0x00007fff61f7287e13 in __libc_start_main (main=0x5555555c3460 <main(int, char**)>, argc=1, argv=0x7fffffffbc8, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffbc8) at /usr/lib/x86_64-linux-gnu/libc-start.c:308
```
Related issues:

Related to Freeciv - Bug #857974: Qt client with -t augmented dumps core (2.... Closed

History

#1 - 2020-01-30 11:18 PM - Chippo Elder

I had the same segment violation while doing the same (inside the Load Game screen and changing your mind and pressing Cancel) thing under gdb.

(gdb) bt full
#0 nation_plural_for_player (pplayer=0x555560eba140) at name_translation.h:123
#1 0x00005555555d7e7c in show_new_turn_info() () at hudwidget.cpp:1664
s = {static null = {<No data fields>}, d = 0x555560022dc0}
ht = <optimized out>
close_list =              {<QListSpecialMethods<hud_text*> = {<No data fields>}, p = {static shared_null = {ref = {atomic = {_q_value = {<std::atomic_base<int> = {static _S_alignment = 4, _M_i = -1}, <No data fields>}}}, alloc = 0, begin = 0, end = 0, array = {0x0}}, d = 0x7ffff71f760 <QListData::shared::null>}, d = 0x7ffff71f760 <QListData::shared::null>}}
research = 0x555555954b60 <research_array>
i = <optimized out>
#2 0x00005555555fb0c3 in qt_start_turn() () at menu.cpp:78
#3 0x00005555555e3601 in qtg_update_timeout_label() () at mapview.cpp:1086
force = 254
#5 0x00005555556e981e in fc_client::slot_disconnect() (this=0x555555fc0580) at fc_client.cpp:497
#6 0x00007ffff71085c8 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#7 0x00007ffff6a1d45e in  () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#8 0x00007ffff6a1e8a3 in  () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#9 0x00007ffff6a1ea65 in QAbstractButton::mouseReleaseEvent(QMouseEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#10 0x00007ffff6928a86 in QWidget::event(QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#11 0x00007ffff698714d in  () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#12 0x00007ffff6989fdc in  () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#13 0x00007ffff6928a86 in QApplicationPrivate::processMouseEvent(QWindowSystemInterfacePrivate::MouseEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#14 0x00007ffff74d19f0 in QGuiApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QWidget**, QPointer<QWidget>&, bool, bool) () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#15 0x00007ffff74d19d3 in QGuiApplicationPrivate::processEvent(QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#16 0x00007ffff74d19e5 in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#17 0x00007ffff74d19f7 in QCoreApplication::exec() () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#18 0x00007ffff74d19f4 in _start () at gui_main.cpp:114
result = <optimized out>
unwind_buf = {cancel_jmp_buf = {{jmp_buf = {0, 4542230881270903410, 93824992692096, 140737488337904, 0, 0, 7664117284589840114, 2021-08-08}}

i = 1
loglevel = LOG_NORMAL
--Type <RET> for more, q to quit, c to continue without paging--c
ui_options = <optimized out>
ui_separator = <optimized out>
option = <optimized out>
fatal_assertions = -1
aii = 1
FUNCTION = "client_main"

#34 0x00007ffff72781e3 in __libc_start_main (main=0x55555555c480 <main(int,char**)>, argc=1, argv=0x7fffffffbf88, init=0x55555555c480, fini=0x55555555c480, stack_end=0x7ffffffb88) at /usr/lib/x86_64-linux-gnu/libc.so.6:205
result = <optimized out>
When a hard to reproduce bug has been caught while running it under gdb, if one had the knowledge, is there more information to be extracted than from a core dump?

#2 - 2020-02-01 01:01 PM - Jacob Nevins
cazf's comment #857974-1 is probably relevant here (same signature shows up in these backtraces).

#3 - 2020-02-01 01:01 PM - Jacob Nevins
- Related to Bug #857974: Qt client with -l augmentedc bumped core (2.6.1+) added

#4 - 2020-04-25 08:21 PM - Marko Lindqvist
- Category set to gui-qt
- Status changed from New to Closed
- Assignee set to Marko Lindqvist

Jacob Nevins wrote:

cazf's comment #857974-1 is probably relevant here (same signature shows up in these backtraces).

Fixed in Bug #857974